Granskning av förbundets informationssäkerhet

Rapport

Nerikes Brandkår

KPMG AB

2020-05-12

Antal sidor 16

Nerikes Brandkår
Granskning av förbundets informationssäkerhet

2020-05-12

Innehållsförteckning

1 Sammanfattning

Vi har av revisorerna i Nerikes Brandkår fått i uppdrag att översiktligt granska förbundets rutiner kring informationssäkerheten. Uppdraget ingår i revisionsplanen för år 2020.Granskningen har syftat till att konstatera om förbundet har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Vår sammanfattande bedömning utifrån granskningens syfte är förbundet inte har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Vi bedömer att förbundets organisation i praktiken är i enlighet MSBs rekommendationer men att det saknas formellt tydliggjorda roller. Det finns upprättade styrdokument för informationssäkerhetsarbetet. Den övergripande informationssäkerhetspolicyn är dock inte uppdaterad sedan 2009 och bör därför ses över för att säkerställa policyns relevans. Avtalet med Nora kommun är övergripande och anger inte tydligt vilka krav som ställs på Nora kommun som IT-leverantör. Vi bedömer att det bör tydliggöras för att säkerställa att den service som ges är anpassad efter förbundets behov. Vi bedömer även att klassningar av förbundets informationstillgångar bör ske för att resurser ska kunna anpassas efter den information som är mest känslig och kritisk. Vår bedömning är även att förbundet bör arbeta fram handlingsplaner för att säkerställa ett systematiskt informationssäkerhetsarbetearbete. Det bör även ytterligare tydliggöras roller och ansvar mellan förbundet och Nora kommun avseende informationssäkerhetsarbetet för att undvika att delar av arbetet förbises. Arbetet med att identifiera och analysera risker bör ske regelbundet för att överensstämma med förbundets nuläge och rådande förutsättningar.

Granskningens bedömningar är delvis baserade på allmänna rekommendationer kring hur organisationer bör bedriva sitt informationssäkerhetsarbete. Det bör därför ställas i relation till förbundets storlek och förutsättningar. Förbundets organisation är relativt liten vilket innebär att föreslagna åtgärder inte behöver kräva ett omfattande arbete för att ett ändamålsenligt informationssäkerhetsarbete ska kunna uppnås.

Utifrån vår bedömning och slutsats rekommenderar vi Direktionen att:

- Genom arbetsordningar eller delegationsordning tydliggöra ansvar för förbundets system.
- Se över förbundets informationssäkerhetspolicy och riktlinjer för informationssäkerhet för att säkerställa dess relevans.
- Utse en informationssäkerhetssamordnare inom förbundet med en tydlig rollbeskrivning.
- I avtalet med Nora kommun tydliggöra gränsdragningarna i ansvarsförhållandena mellan förbundet och Nora kommun. Det bör inkludera att genom SLA tydliggöra kravställandet på Nora kommun som IT-leverantör.
- Framarbeta en rutin för behörighetskontroller.
- Utveckla kortsiktiga mål för informationssäkerhetsarbetet med tillhörande handlingsplaner.

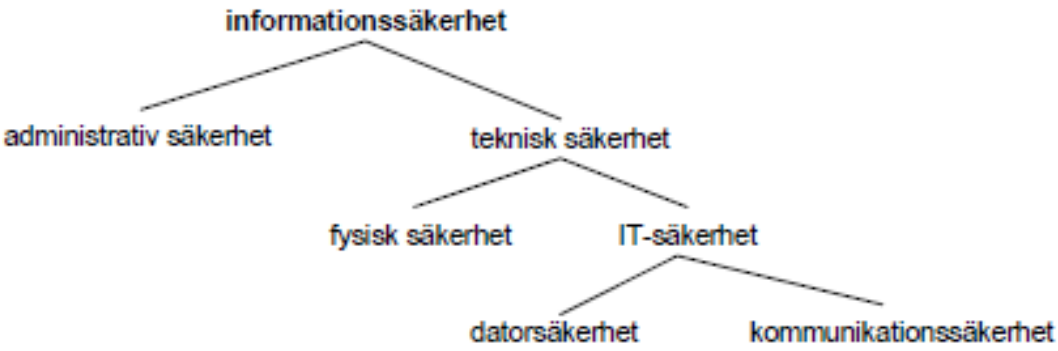
- Säkerställa att arbetet med att identifiera och analysera risker sker regelbundet.

2 Inledning/bakgrund

Vi har av revisorerna i Nerikes Brandkår fått i uppdrag att översiktligt granska förbundets rutiner kring informationssäkerheten. Uppdraget ingår i revisionsplanen för år 2020.

Informationssäkerhet är ett begrepp som används om säkerhet för information som hanteras i förbundets IT-system. Allt mer information hanteras idag med olika tekniska lösningar och aldrig förr har offentlig sektor hanterat sådana mängder information som görs idag. Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod.

Informationssäkerhet innebär att skydda information utifrån dess krav på konfidentialitet, riktighet och tillgänglighet i alla förbundets system. För att kunna hantera detta på ett ändamålsenligt sätt krävs att förbundet har ett systematiskt informationssäkerhetsarbete där flera funktioner är involverade och rätt organiserade för uppdraget. IT-säkerhet är inte en IT-fråga utan en fråga om att säkra och trygga driften av förbundets kärnverksamhet.



Bilden ovan illustrerar de olika begreppens relation till varandra.

Nerikes Brandkår köper idag den tekniska IT-tjänsten av Nora kommun vilket ställer ytterligare krav på att verksamheten har fastställda rutiner och tar ansvar för sin information och informationssäkerhet även i relation till extern part som leverantör av IT-infrastrukturen.

Revisorerna bedömer risken att det systematiska informationssäkerhetsarbetet inte är ändamålsenligt och att det finns risk för brister i förbundets organisering och arbetssätt inom området, inte minst i relation till extern leverantör av IT-infrastruktur.

Med anledning av ovanstående drar förbundets revisorer slutsatsen i sin riskanalys, att förbundets rutiner avseende informationssäkerheten behöver granskas.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen syftar till att konstatera om förbundet har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Granskningen ska besvara följande revisionsfrågor:

— Finns en ändamålsenlig organisation för att arbeta med informations-säkerhetsfrågorna i förbundet?
— Finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet dokumenterat och förankrad i förbundets verksamheter?
— Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet (förbundet) och IT-organisation (Nora kommun)?
— Arbetar förbundet systematiskt med att identifiera och analysera risker för informationssäkerheten?
— Vilka krav har ställts på Nora kommun som leverantör av IT-tjänster, varför har valet fallit på Nora kommun som leverantör?
— Finns det en uppföljning av kvalitet av IT-tjänsterna?

Granskningen omfattar Direktionen och dess ansvar för informationssäkerheten inkl rollen som kravställare på extern leverantör.

Granskningen avser direktion i Nerikes Brandkår.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

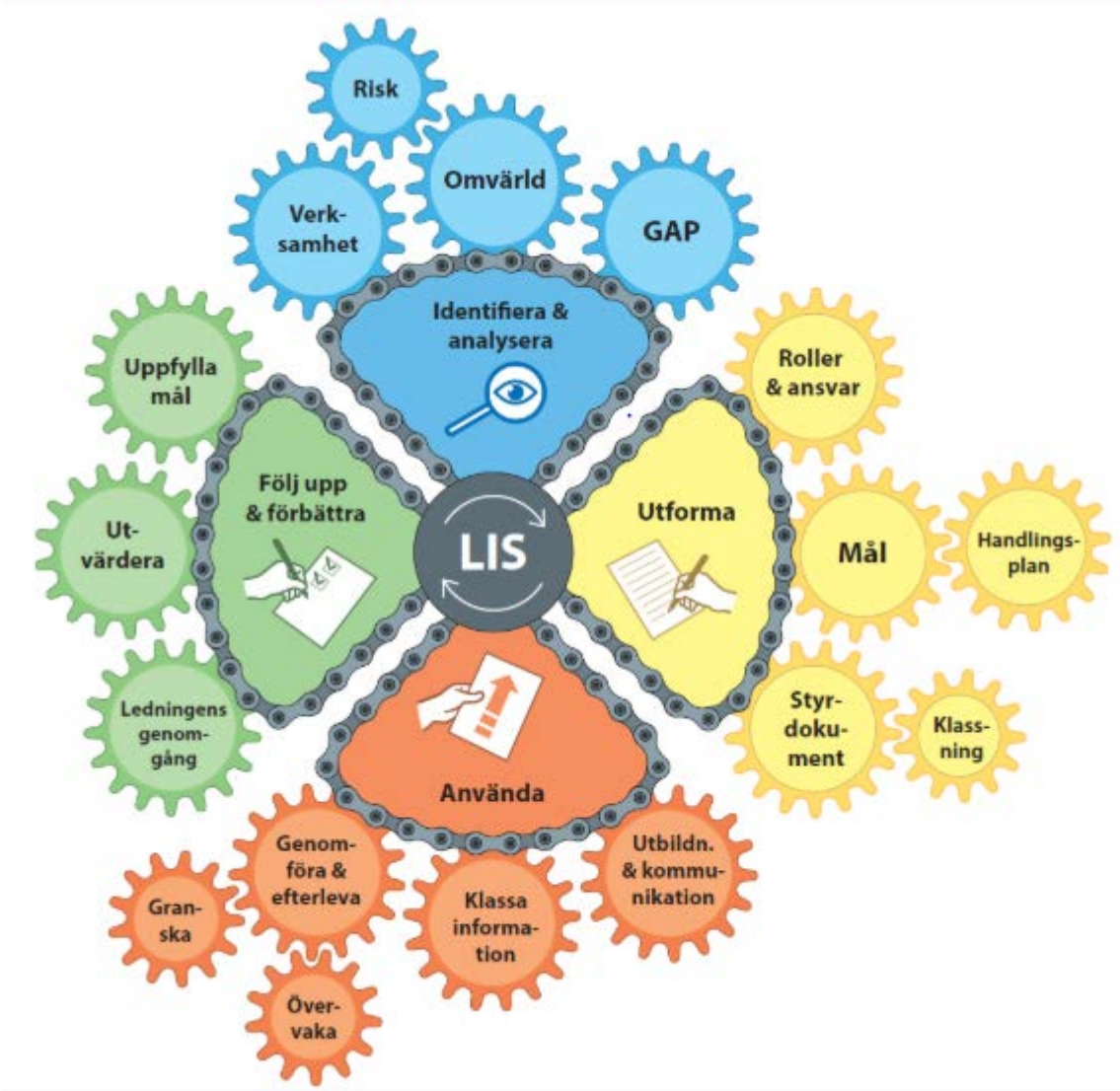
— Tillämpbara interna regelverk, policys och beslut
— MSBs rekommendationer avseende Ledningssystem för informationssäkerhet
— NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker

2.2.1 MSB:s metodstöd

MSB[1] har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet är baserat på den internationella standard-serien för informationssäkerhet, ISO/ IEC 27000 och ämnar till att förtydliga hur informationssäkerhetsarbetet kan utformas.

Metodstödet består av fyra olika metodsteg för informationssäkerhetsarbetet vilka illustreras i nedanstående figur.

[1] Myndigheten för Samhällsskydd och Beredskap



Metodstödet och de fyra metodstegen med underliggande metoddelar.

2.2.1.1 Identifiera och analysera

Syftet med att analysera avseende informationssäkerhetsarbetet är enligt MSB att säkerställa att informationssäkerheten utformas utifrån verksamhetens rådande förutsättningar. Det ska även leda till att väsentliga informationstillgångar identifieras, vilka risker de ska skyddas mot, samt valda säkerhetsåtgärder.

2.2.1.2 Utforma

Enligt MSB:s metodstöd behövs följande delar för ett systematiskt informationssäkerhetsarbete:

- Organisation

- Informationssäkerhetsmål
- Styrdokument
- Klassningsmodell
- Handlingsplan
- Kontinuitetshantering för informationstillgångar

2.2.1.3 Använda

När verksamheten har utformat styrningen enligt avsnitt 3.1.2 ska det tillämpas. Det innebär:

- Kontinuerligt arbete med att klassa organisationens information för att identifiera känslig och kritisk information för att kunna säkerställa tillräckligt skydd.
- Genomföra och efterleva de handlingsplaner och styrdokument som avser informationssäkerhetsarbetet
- Utbilda och kommunicera informationssäkerhetsfrågor till organisationens medarbetare. Det är ständigt pågående arbete som är nödvändigt för att skapa ett systematiskt informationssäkerhetsarbete.

2.2.1.4 Följa upp och förbättra

Informationssäkerhetsarbetet ska utvärderas och följas upp för att säkerställa att arbetets fortsatta lämplighet, tillräcklighet och verkan. Det kan enligt MSB ske genom övervakning, mätning och måluppföljning.

2.3 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer/avstämningar med berörda tjänstemän.

Rapporten är faktakontrollerad av samtliga intervjuade.

3 Resultat av granskningen

3.1 Styrdokument

För Nerikes Brandkår finns en informationssäkerhetspolicy som styr förbundets arbete med informationssäkerhet. Följande mål anges i policyn:

- skydda den personliga integriteten
- bevara ett högt förtroende hos medborgarna
- säkerställa att gällande lagar och bestämmelser följs
- förhindra eller minska effekterna av störningar och skador

- skydda information och informationssystem mot bedömda hot
- skapa ordning och kontroll över Nerikes Brandkårs informationsbehandling

Utifrån policyn har riktlinjer för informationssäkerhet tagits fram[2]. Riktlinjerna omfattar bl.a. informationsklassning, roller och ansvar, fysisk säkerhet, kommunikation, åtkomst till program och nätverk, loggning av IT-resurser, kontinuitetsplanering, intern kontroll samt användning av internet, epost, fax och telefoni.

Enligt MSBs metodstöd bör informationssäkerhetspolicyn ej uppdateras årligen då det är ett strategiskt dokument som avser viljeriktningen med informationssäkerheten. Samtidigt beskrivs informationssäkerhet som ett föränderligt område, vilket innebär att den riskerar att bli förlegad om den uppdateras för sällan. En rimlig livslängd på en informationssäkerhetspolicy är enligt MSB ca. 3–5 år. Nerikes Brandkårs informationssäkerhetspolicy är antagen av Direktionen 2009-04-16.

Av våra dialoger framgår att det finns planer på att uppdatera informationssäkerhetspolicyn men att man avvaktar att IT-leverantören Nora kommun uppdaterar sina styrdokument i syfte att samordna.

3.2 Organisation

3.2.1 Organisation för informationssäkerhet enligt MSBs metodstöd

I MSB:s metodstöd för systematiskt informationssäkerhetsarbete framgår hur ansvaret för arbetet med informationssäkerhet bör fördelas[3].

Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, verksamhetschefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten.

Det är viktigt att tydligt klargöra informationssäkerhetssamordnaren roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på, enligt MSB:s metodstöd, på organisationens struktur men bör generellt vara placerad nära ledningen, exempelvis i en ledningsstab.

3.2.2 Nerikes Brandkårs organisation för informationssäkerhetsarbetet

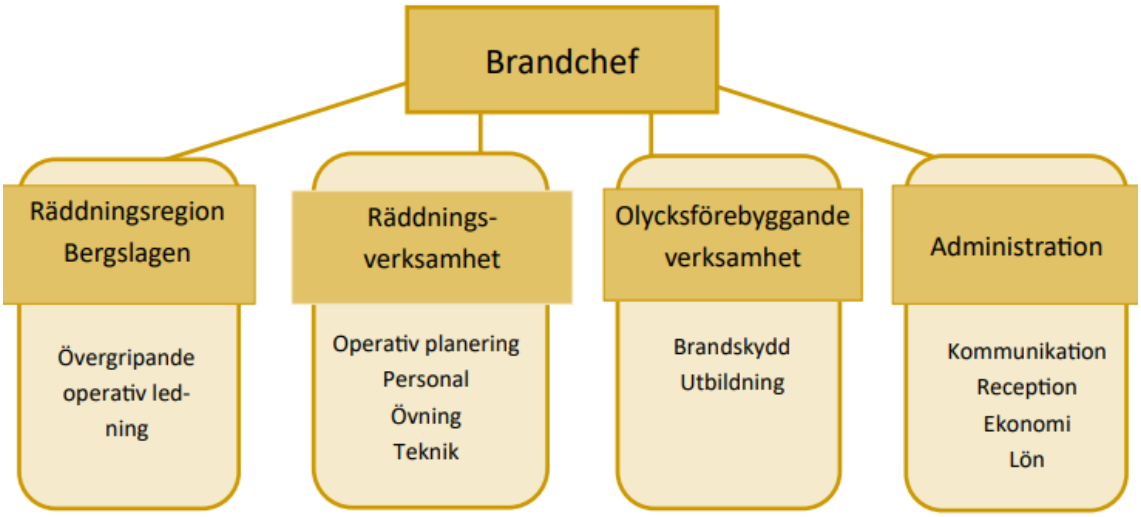
Enligt förbundets riktlinjer är Direktionen ytterst ansvarig för förbundets informationssäkerhet. De styr genom fastställandet av gällande säkerhetskrav för verksamheten samt fastställandet av informationssäkerhetspolicyn.

[2] Antagen av direktionen 2009-04-16
[3] Avser en generell organisation. Enheter och likande i exemplet är inte direkt applicerbara på Nerikes Brandkårs organisation.

Vidare framgår att alla medarbetare inom förbundet ska känna till att de har ett ansvar för brandkårens informationssäkerhet samt att följa regler och anvisningar. Vidare har varje anställd skyldighet att rapportera funktionsstörningar och fel i system, utrustningar och data.

Av våra intervjuer framgår att förbundet inte har en formellt ansvarig informationssäkerhetssamordnare. I praktiken uppges dock en av förbundets två vice brandchefer ansvara för informationssäkerhetsfrågorna i och med sitt ansvar för förbundets förebyggande verksamhet och IT-verksamhet.

Enligt våra intervjuer finns det inte någon formellt ansvarig för förbundets olika system. Det är respektive chef som i praktiken enligt uppgift ansvarar för de system som dennes verksamhet använder. Vi har inte tagit del av någon arbetsordning eller liknande dokument som fastställer verksamhetschefers systemansvar. Det uppges vara cirka 35 stycken systemanvändare i förbundet på daglig basis. Enligt våra avstämningar är det vice brandchef samt förbundets ekonomichef ytterst tar ansvar för förbundets verksamhetssystem.



Organisationsschema för Nerikes brandkår. Vice brandchef med informellt ansvar för informationssäkerhet organiseras under ”Olycksförebyggande verksamhet.

3.2.3 IT-organisation

Nerikes Brandkår har handlat upp sitt IT-stöd av Noras kommun. Utöver det har förbundet handlat upp ett antal system som Nora kommun inte är involverade i. Där står respektive leverantör för IT-supporten. Vi har tagit del av det avtal Nerikes Brandkår har upprättat med Nora kommun avseende IT-support. Avtalet med Nora kommun trädde i kraft 2010-01-01. Enligt våra intervjuer med företrädare för förbundet ser man positivt på den service som ges av Nora kommun i rollen som IT-leverantör. Att Nora är en liten kommun lyfts som en fördel då det upplevs finnas en förståelse för de båda parternas förutsättningar. Vidare upplever förbundet att den service som Nora kommun levererar är hög i förhållande till kostnaden.

Av avtalet framgår att det omfattar support till användare samt driftstöd server, backup. Enligt avtalet ska Nora kommun vara tillgängliga för support på vardagar 08.30-11.30 och 12.30-16.00. Det framgår av våra intervjuer att Nora även har bistått med support på helgdagar och andra tider som ej omfattas av avtalet. Ibland inom knappa tidsramar. Det har enligt intervjuer heller inte upprättats någon specifik SLA[4] för förbundets system. Vi har heller inte tagit del av något annat dokument som tydliggör olika nivåer av service baserat på hur kritiska systemen bedöms vara.

3.2.3.1 Uppföljning

Enligt intervjuer genomförs regelbundet avstämningar med Nora kommun avseende kvalitet på IT-tjänsterna. Enligt intervjuer brukar avstämningarna kretsa kring IT-utveckling och inte fokuserat på informationssäkerhet även om det har berörts. Däremot informerar Nora kommun om vad som är aktuellt, vilket även innefattar informationssäkerhet. Vi har inte tagit del av någon skriftlig uppföljning.

3.2.4 Bedömning

Finns en ändamålsenlig organisation för att arbeta med informations-säkerhetsfrågorna i förbundet?

Utifrån dokumentstudier och intervjuer kan vi konstatera att det i praktiken är verksamhetsansvarig som ansvarar för de system som används inom respektive område. Vi konstaterar även att det informellt finns en samordnare för informationssäkerhetsarbetet. Det är i enlighet med MBS:s rekommendationer om att ansvaret för informationssäkerheten ska följa den ordinarie ansvarsfördelningen i verksamheten. Vi ser däremot en risk i att de olika rollernas ansvar ej har formaliserats. Vår bedömning är att ansvaret bör formaliseras för de verksamhetschefer som ska vara systemansvariga. Vi bedömer även att en informationssäkerhetsamordnare bör utses för att tydliggöra organisationen och skapa förutsättningar för ett systematiskt informationssäkerhetsarbete.

Vidare finns det en upprättad informationssäkerhetspolicy i förbundet. Baserat på policyn har riktlinjer tagits fram. Informationssäkerhetspolicyn har inte uppdaterats på ca 11 år att jämföra med MSB:s rekommendationer om 3-5 år. Vi ser positivt på att det finns planer inom förbundet på att utveckla nya styrdokument men konstaterar att det vid tidpunkten för granskningen ej genomförts. Vi bedömer att informationssäkerhetspolicy och riktlinjer bör uppdateras för att säkerställa dokumentens relevans.

Vilka krav har ställts på Nora kommun som leverantör av IT-tjänster, varför har valet fallit på Nora kommun som leverantör?

Enligt intervjuer föll valet på Nora kommun som leverantör eftersom man upplever en förståelse i Nora för förbundets förutsättningar då både Nora och Nerikes Brandkår är mindre organisationer. Vi konstaterar att det finns ett upprättat avtal med Nora kommun avseende IT-tjänster. Avtalet är övergripande och innefattar ej SLA för förbundets

[4] Står för ”Service Level Agreement” och anger den nivå av service som ska vara tillgänglig för respektive system.

system. Vidare kan vi utifrån våra intervjuer konstatera att Nora kommun levererar tjänster till förbundet på andra tider än de som anges i avtalet. Vi ser en risk för otydlighet avseende vilken service som Nora kommun förväntas leverera. Det riskerar leda till att Nora i egenskap av leverantör ej har anpassade resurser för den nivå av service förbundet kräver. Vi bedömer därför att Nerikes brandkårs krav på Nora kommun som leverantör av IT-tjänster bör konkretiseras.

Finns det en uppföljning av kvalitet av IT-tjänsterna?

Enligt intervjuer genomförs avstämningar med Nora kommun i egenskap av IT-leverantör regelbundet två gånger om året. Det upplevs dock vara väldigt detaljorienterade och inte fokusera på informationssäkerhet. Av intervjuerna framgår att frågorna som lyfts till stor del är på Nora kommuns initiativ och inte drivet av Nerikes brandkår i egenskap av beställare.

3.3 Informationssäkerhetsarbete

3.3.1 Säkerhetsklassningar

Det varierar hur kritisk och känslig olika typer av information är för en organisation. Därför är det viktigt att genomföra en bedömning utav vad som är lämplig nivå av säkerhet och skydd för olika typer av information. Enligt MSBs metodstöd bör informationen klassas utifrån konfidentialitet, riklighet och tillgänglighet.

Av förbundets riktlinjer framgår att verksamhetsansvariga inom Nerikes Brandkår ansvarar för att informationen inom deras respektive verksamhetsområde hanteras på ett korrekt sätt och att det både bedöms och ges korrekt stöd.

Vidare ska, enligt förbundets riktlinjer, även ny personal med tillgång till särskild information genomgå en lämplighetsprövning. Det gäller även entreprenörer och tillfällig personal.

Enligt våra intervjuer görs ingen klassning av förbundets informationstillgångar. Det finns heller ingen fastställd modell för klassning i förbundet.

3.3.2 Kontinuitetsplanering

Kontinuitetsplanering syftar på den planeringsprocess som ska säkerställa fortsatt verksamhet vid störningar och avbrott i den ordinäre IT-driften. Enligt förbundets riktlinjer ska det finnas en avbrottsplan vilken utgör den sammanfattande beteckningen på de åtgärder som ska säkerställa fortsatt verksamhet i händelse av störning samt möjliggöra återstart av IT-driften. Respektive systemägare ansvarar för framtagandet av avbrottsplaner. Dataansvarig ansvarar för de system där det inte har utsetts någon systemägare. I samband med framtagandet av respektive systemsäkerhetsintroduktion ska kraven på systemets tillgänglighet fastställas. Där ska det framgå den längsta tid som ett datasystem får vara obrukbart innan verksamheten äventyras.

Av våra intervjuer framgår att Nora kommun löser mycket av problemen med IT ”på studs” och att det ej är utarbetat efter specifika avbrottsplaner.

3.3.3 Logg- och behörighetskontroller

Nerikes brandkår har dokumenterade riktlinjer avseende Loggning av IT-resurser. Enligt riktlinjerna sker loggning i syfte att upptäckta avvikelser avseende riktlinjerna för informationssäkerhet. Av riktlinjerna framgår vad som gäller avseende skydd av den personliga integriteten, åtkomst till loggresultat, klocksynkronisering samt skyldighet att vidta åtgärder.

Avseende behörighet står det i förbundets riktlinjer för informationssäkerhet att ej giltiga behörigheter regelbundet ska regelbundet tas bort för att undvika att persona som avslutat sin anställning eller bytt arbetsuppgifter finns kvar i systemen.

Enligt intervjuer beställarförbundet logg- och behörighetskontroller av Nora kommun. Vidare framgår att det utöver beställningarna till Nora kommun inte görs kontroller. Därmed görs ingen regelbunden kontroll.

3.3.4 Intern kontroll och riskanalyser

Enligt riktlinjerna är kontroll av förbundets efterlevnad av riktlinjerna för informationssäkerhet en del av brandkårens internkontroll. Vilka områden rörande informationssäkerhet som ska kontrolleras fastställs årligen av direktionen. Exempel på kontrollområden är:

- Administrativ säkerhet
- Fysisk säkerhet
- Logisk säkerhet

Metoder som används kan exempelvis vara enkäter, intervjuer, hot- och riskanalyser eller penetrationstester.

I de fall brister upptäcks ska förslag till handlingsplan upprättas.

Det framgår av våra intervjuer att Nora kommun genomför kontroller avseende teknisk säkerhet. Dock genomförs exempelvis inte penetrationstester vilket enligt intervjuer beror på knappa resurser.

Avseende administrativ säkerhet uppges exempel på kontroller vara:

- Kunskap om och efterlevnad av fastställda riktlinjer inom Nerikes Brandkår för informationssäkerhet på såväl ledningsnivå som användarnivå.
- Efterlevnad av lagstiftning inom området.

Enligt definitionen av informationssäkerhet är administrativ säkerhet en del av informationssäkerhet men inte teknisk säkerhet och IT-säkerhet. Av våra intervjuer görs det tydligt att Nora kommun uppfattar att deras uppdrag innefattar teknisk säkerhet men inte informationssäkerhet.

Det framgår av förbundets uppföljning av internkontrollplan 2019[5] att det under 2019 genomfördes en kontroll av rutiner gällande GDPR. Vi noterar att samma punkt fanns med även i 2018 års intern kontrollplan. Baserat på kontrollen har riktlinjer för personuppgiftshantering upprättats. I övrigt finns ingen kontrollpunkt avseende informationssäkerhet med i förbundets internkontrollplan 2018 eller 2019.

Enligt våra intervjuer genomfördes en större riskanalys på verksamhetsövergripande nivå omkring år 2000. Sedan dess har ingen större riskanalys genomförts.

3.3.5 Utbildning

Enligt förbundets riktlinjer bör alla som använder brandkårens IT-system ges en grundläggande informationssäkerhetsutbildning. Den bör innehålla följande områden:

- Viktiga delar av Nerikes Brandkårs riktlinjer för informationssäkerhet
- Aktuell lagstiftning och säkerhetsföreskrifter
- Säkerhetsåtgärder som används inom organisationen

Av våra intervjuer framgår att en grundläggande utbildningen erbjuds nya medarbetare och även övriga medarbetare regelbundet ska ges uppdaterad information. Det sker enligt uppgift sällan. Däremot uppges det faktum att förbundet inte har så stort antal regelbundna systemanvändare leda till informell kunskapsspridning.

3.3.6 Måluppfyllelse

Som tidigare beskrivit finns övergripande mål för informationssäkerhetsarbetet formulerade i förbundets informationssäkerhetspolicy. Vi har ej vid tidpunkten för granskningen tagit del av någon dokumenterad uppföljning avseende målen för informationssäkerheten. Enligt är MSB är det ej nödvändigt att samtliga strategiska mål är mätbara men att det bör kunna påvisas progression.

Enligt MSB bör det utöver långsiktiga mål (formulerade i informationssäkerhetspolicyn) finnas kortsiktiga mål. De kortsiktiga målen bör arbetas in en handlingsplan och följas upp årligen. Vi har ej tagit del av någon handlingsplan eller kortsiktiga mål för förbundets informationssäkerhetsarbete.

3.3.7 Bedömning

Finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet dokumenterat och förankrad i förbundets verksamheter?

Utifrån intervjuer och genomgång av informationssäkerhetspolicy, tillhörande riktlinjer och internkontrollplaner kan vi konstatera att det genomförs utbildningar inom informationssäkerhet för förbundets medarbetare. Vi kan vidare konstatera att det vidtas åtgärder för ett antal andra området enligt riktlinjerna för informationssäkerhet, exempelvis behörighetskontroller. Enligt intervjuer sker detta genom beställning till Nora kommun. Vi har inte tagit del av någon rutin för behörighetskontroller. Vi ser en risk för gamla behörigheter ligger kvar i systemen om det inte regelbundet kontrolleras.

[5] Godkänd av Direktionen 2020-03-05

Vi kan även konstatera att det inte finns någon modell för att klassa förbundets informationstillgångar. Vår bedömning är att informationen bör klassas för att skydd ska kunna anpassas efter hur kritisk och känslig informationen är. Därmed kan även onödiga kostnader för överskydd undvikas för icke kritisk information.

Vidare finns inga handlingsplaner upprättade i syfte att konkretisera informationssäkerhetsarbetet. Vår bedömning är att det bör upprättas i syfte att tydliggöra informationssäkerhetsarbetet och säkerställa ett systematiskt informationssäkerhetsarbete.

Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet (förbundet) och IT-organisation (Nora kommun)?

Det finns som tidigare nämnt ett avtal upprättat för IT-support mellan Nerikes Brandkår och Nora kommun där servicenivån på Nora kommun som leverantör inte är tydliggjord. Enligt intervjuer genomför Nora kommun en del kontroller avseende teknisk säkerhet men inte för administrativ säkerhet som är en del av den bredare definition informationssäkerhet. Genom granskning av förbundets internkontrollplaner kan vi konstatera att kontroller av regelefterlevnad av GDPR har genomförts av förbundet. Vår bedömning är dock att roller och ansvar bör tydliggöras för att undvika risken för att delar av informationssäkerhetsarbetet förbises.

Arbetar förbundet systematiskt med att identifiera och analysera risker för informationssäkerheten?

Enligt intervjuer har ingen övergripande riskanalys genomförts sedan ca år 2000. Det genomförs även som tidigare konstaterat en del kontroller i och med den interna kontrollen. Vår bedömning är att det delvis pågår ett arbete med att identifiera och analysera risker för informationssäkerheten. Däremot sker det inte systematiskt. Därför bedömer vi att arbetet med att identifiera och analysera risker bör intensifieras och kontinuerligt följas upp för att säkerställa att analysen överensstämmer med förbundets nuläge.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att förbundet inte har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Vi bedömer att förbundets organisation i praktiken är i enlighet med MSBs rekommendationer men att det saknas formellt tydliggjorda roller. Det finns upprättade styrdokument för informationssäkerhetsarbetet. Den övergripande informationssäkerhetspolicyn är dock inte uppdaterad sedan 2009 och bör därför ses över för att säkerställa policyns relevans. Avtalet med Nora kommun är övergripande och anger inte tydligt vilka krav som ställs på Nora kommun som IT-leverantör. Vi bedömer att det bör tydliggöras för att säkerställa att den service som ges är anpassad efter förbundets behov. Vi bedömer även att klassningar av förbundets informationstillgångar bör ske för att resurser ska kunna anpassas efter den information som är mest känslig och kritisk. Vår bedömning är även att förbundet bör arbeta fram handlingsplaner för att säkerställa ett systematiskt informationssäkerhetsarbetearbete. Det bör även ytterligare tydliggöras roller och

ansvar mellan förbundet och Nora kommun avseende informationssäkerhetsarbetet för att undvika att delar av arbetet förbises. Arbetet med att identifiera och analysera risker bör ske regelbundet för att överensstämma med förbundets nuläge och rådande förutsättningar.

Granskningens bedömningar är delvis baserade på allmänna rekommendationer kring hur organisationer bör bedriva sitt informationssäkerhetsarbete. Det bör därför ställas i relation till förbundets storlek och förutsättningar. Förbundets organisation är relativt liten vilket innebär att föreslagna åtgärder inte behöver kräva ett omfattande arbete för att ett ändamålsenligt informationssäkerhetsarbete ska kunna uppnås.

4.1 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi Direktionen att:

- Genom arbetsordningar eller delegationsordning tydliggöra ansvar för förbundets system.
- Se över förbundets informationssäkerhetspolicy och riktlinjer för informationssäkerhet för att säkerställa dess relevans.
- Utse en informationssäkerhetssamordnare inom förbundet med en tydlig rollbeskrivning.
- I avtalet med Nora kommun tydliggöra gränsdragningarna i ansvarsförhållandena mellan förbundet och Nora kommun. Det bör inkludera att genom SLA tydliggöra kravställandet på Nora kommun som IT-leverantör. Samt att tydliggöra ansvar avseende informationssäkerhetsarbetet för att undvika att delar förbises.
- Framarbeta en rutin för behörighetskontroller.
- Utveckla kortsiktiga mål för informationssäkerhetsarbetet med tillhörande handlingsplaner.
- Säkerställa att arbetet med att identifiera och analysera risker sker regelbundet.

Datum som ovan

KPMG AB

Sara Linge
Certifierad kommunal yrkesrevisor

Daniel Strandberg
Kommunal revisor

Nerikes Brandkår
Granskning av förbundets informationssäkerhet

2020-05-12